ABSTRACT

A wide-blocksize block cipher that takes a possibly long string as plaintext and turns it into a ciphertext having the same length as the plaintext. Every bit of the ciphertext strongly depends on every bit of the plaintext. The wide-blocksize block cipher is made from a conventional block cipher, which is a block cipher that operates on strings of some small, fixed length. The wide-blocksize block cipher is obtained from the conventional block cipher by a three-step process. The first step is to encipher the plaintext using some mode of operation of the conventional block cipher. The second step is to mask the resulting intermediate value by way of a computationally cheap mixing step. The third step is to decipher the masked intermediate value using some mode of operation of the conventional block cipher. The specified steps may depend on a non-secret tweak, so that the wide-blocksize block cipher becomes tweakable. The method can be used for disk-sector encryption, to securely store user data on a mass-storage device.